

Koncepcja ochrony danych

Lokalna wersja szkolna

Przetwarzanie, ochrona i prawa

Żadnych zapisanych nagrań dźwiękowych. Żadnych profili głosowych.

Imiona i nazwiska z klasy, prywatne wypowiedzi i uwagi niezwiązane z przedmiotem są filtrowane przed zapisaniem notatek edukacyjnych. Przegląd przez nauczycieli jest opcjonalny.

Wszystkie pliki i dane lokalnej instalacji szkolnej są szyfrowane podczas przechowywania i przesyłania. Szkoła określa okres przechowywania treści edukacyjnych; standardem jest jeden rok szkolny.

Niniejszy dokument opisuje **lokalną wersję szkolną ContextFriend**: przetwarzanie, środki ochrony i prawa. Podczas wdrożenia w szkole każda instalacja jest sprawdzana i dokumentowana na podstawie niniejszej koncepcji.

Szkoła będąca administratorem danych uzupełnia własne dane kontaktowe, podstawy prawne, funkcje i terminy usunięcia. Niniejsza ogólna koncepcja produktu nie zastępuje ani jej informacji o ochronie danych, ani wymaganej oceny skutków dla ochrony danych, ani umowy o przetwarzanie w imieniu administratora (art. 28 RODO).

W niniejszej pełnej koncepcji ochrony danych

Odpowiedzialność i podstawy prawne · Strona 2

Przetwarzanie i filtrowanie · Strona 4

Dostęp i dalsze środki ochrony · Strona 6

Odbiorcy i konserwacja · Strona 8

Wersja, dowody i źródła · Strona 10

Rodzaje danych i cele · Strona 3

Szyfrowanie · Strona 5

Okresy przechowywania i usuwanie · Strona 7

Prawa i incydenty ochrony danych · Strona 9

Wersja skrócona: osobno na stronie ochrony danych

Dostawca i wydawca

TamerinTECH GmbH

Seestr. 19

83727 Schliersee

Germany

Telefon: +49 8026 387 25 98

hello@context-friend.com

www.tamerin.tech

Dyrektor zarządzający: Ron Tamerin

Odpowiedzialny za treść: Ron Tamerin

Adres jak obok

Sąd rejestrowy: Amtsgericht München

Rejestr handlowy: HRB 263667

Numer VAT UE: DE340834936

Punkt kontaktowy ds. ochrony danych: hello@context-friend.com

[Pełny Impressum na stronie](#)

Odpowiedzialność i dopuszczalność

1. Zakres obowiązywania

Lokalna wersja szkolna służy do utrwalania materiału z określonych jednostek lekcyjnych. Tworzy przedmiotowe notatki edukacyjne, udostępnia do wykorzystania zgodnie z prawem dostarczone materiały i umożliwia, o ile szkoła na to zezwala, zadawanie pytań lokalnej AI. Rozpoznawanie mowy, filtrowanie, AI, wyszukiwanie, zarządzanie kontami i przechowywanie odbywają się na serwerze szkoły.

Wymogi dotyczą wszystkich osób, których dane są przy tym przetwarzane: uczniów, nauczycieli, asystentów szkolnych, osób zastępujących i innych obecnych oraz uprawnionych rodziców i opiekunów prawnych. Samo odwiedzanie strony internetowej i formularze kontaktowe są opisane osobno w [polityce prywatności publicznej strony internetowej](#).

2. Administrator danych i kontakty w sprawach ochrony danych

Szkoła: Administratorem danych w rozumieniu RODO jest szkoła lub podmiot wskazany w jej szkolnych informacjach. Decyduje on o celu, podstawie prawnej, zakresie, kręgu użytkowników, okresach przechowywania i eksploatacji. Dyrekcja szkoły organizuje dopuszczenie do użytku; szkolny inspektor ochrony danych (IOD) doradza i niezależnie nadzoruje. Organ odpowiedzialny za utrzymanie szkoły (Schulaufwandsträger) oraz dział IT szkoły przejmują odpowiednio ustalone zadania eksploatacyjne.

Dostawca: TamerinTECH GmbH dostarcza produkt. Sama rola dostawcy nie daje dostępu do danych z lekcji. W przypadku zleconego przetwarzania danych osobowych, na przykład w ramach wsparcia technicznego, TamerinTECH działa wyłącznie na polecenie administratora i na podstawie wymaganej umowy zgodnie z art. 28 RODO.

Kontakt: Szkoła publikuje swój adres oraz służbowy kontakt swojego inspektora ochrony danych przed rozpoczęciem korzystania. Zapytania dotyczące ochrony danych kierowane do TamerinTECH docierają do punktu kontaktowego pod adresem hello@context-friend.com lub na adres dostawcy podany na stronie 1. Punkt kontaktowy nie jest automatycznie formalnie wyznaczonym inspektorem ochrony danych. Wymagane wyznaczenie i podanie jego danych kontaktowych następują osobno zgodnie z art. 37 RODO i § 38 BDSG (niemiecka federalna ustawa o ochronie danych).

3. Podstawy prawne i wymagane informacje

W przypadku państwowych szkół bawarskich należy zbadać w szczególności art. 6 ust. 1 lit. e i ust. 3 RODO, [art. 85 BayEUG](#) (bawarska ustawa o oświacie) oraz [§ 46 BaySchO z załącznikiem 1](#) (bawarskie rozporządzenie szkolne). Nie wynika z tego ogólne zezwolenie na stałe rejestrowanie lekcji. Przetwarzanie mowy, pamięć edukacyjna, dostępy i dzienniki bezpieczeństwa podlegają każdorazowo badaniu pod kątem niezbędności i odpowiednich alternatyw.

W przypadku funkcji dobrowolnych wymagana zgodę należy uzyskać w sposób konkretny, świadomy, dobrowolny i z możliwością wycofania na przyszłość. Szkoła ustala kwestię reprezentacji osób niepełnoletnich, równoważną alternatywę bez żadnej niekorzyści oraz prawa pracowników do współdecydowania. Zalogowanie się i przeczytanie niniejszego dokumentu nie zastępują zgody.

Szczególne kategorie danych osobowych, na przykład informacje o stanie zdrowia, nie są celowo zbierane. Jeżeli ich przetwarzanie jest nieuniknione, należy dodatkowo przestrzegać art. 9 RODO; w braku solidnej podstawy rejestrowanie należy wstrzymać. Należy również przestrzegać prawa do wypowiedzianego słowa.

Rodzaje danych i cele

4. Jakie dane są przetwarzane

Kategoria danych	Treść, cel i granica
Mowa	Mowa podczas wyrażnie aktywowanych fragmentów lekcji w celu lokalnego przekształcenia w tekst. Głosy nigdy nie są zapisywane jako plik audio, archiwizowane ani zabezpieczane w kopii zapasowej. Brak odtwarzania, brak profilu głosowego.
Nieprzetworzony tekst	Rozpoznany dosłowny tekst wyłącznie do lokalnego filtrowania treści. Odrzucany po filtrowaniu, najpóźniej pięć minut po zarejestrowaniu. Brak trwałego zapisu, brak źródła wyszukiwania i brak kopii zapasowej.
Notatki edukacyjne i materiały	Przedmiotowe wyjaśnienia, przykłady, zadania, odniesienia do źródeł oraz dokumenty dopuszczalnie udostępnione przez szkołę. Cel: utrwalanie i powtarzanie w uprawnionym kursie.
Dane wyszukiwania i dane pochodne	Fragmenty tekstu, lokalne indeksy wyszukiwania, embeddingi i powiązania przedmiotowe. Otrzymują te same uprawnienia i terminy usunięcia co ich źródła.
Pytania i odpowiedzi	Własne wpisy, odpowiedzi i kontekst rozmowy dotyczący danego pytania edukacyjnego. Trwała historia jest prowadzona wyłącznie za zezwoleniem szkoły i jest wcześniej wyjaśniana. Brak ogólnego wglądu innych uczniów.
Dostępny i uprawnienia	Niezbędne identyfikatory, chronione dane logowania, role, przypisania do kursów i wymagane zezwolenia. Brak publicznego katalogu osób; brak zbierania na zapas prywatnych danych profilowych.
Dane bezpieczeństwa	Niezbędne zdarzenia logowania, dostępu i administracyjne, w stosownych przypadkach adresy IP i znaczniki czasu. Cel: ochrona dostępu i wyjaśnianie błędów. Brak tekstów lekcji, treści czatów ani tajnych danych dostępowych w dziennikach.
Kopie zapasowe	Zaszyfrowane kopie wyrażnie dopuszczonych zapisanych zasobów do celów przywracania. Brak kopii audio ani surowego tekstu; ograniczone prawa dostępu i czas przechowywania.

4.1 Pochodzenie danych i odniesienie do osób

Dane powstają w aktywowanych fragmentach lekcji, poprzez własne wpisy, szkolne przypisania do kursów i udostępnione materiały. W przypadku obcych źródeł danych szkoła podaje wymagane informacje zgodnie z art. 14 RODO. Sama możliwość przetwarzania danych nie jest zezwoleniem na zbieranie wszystkich kategorii danych.

Głos, treść pytania, identyfikator lub kontekst mogą umożliwić rozpoznanie osoby. Filtry imion i nazwisk oraz pseudonimy nie stanowią pełnego dowodu anonimowości. Stwierdzenie o usuniętych imionach i nazwiskach odnosi się do notatek edukacyjnych, a nie do niezbędnych danych konta ani ustawowych dowodów szkoły.

4.2 Wykluczone analizy

Żadnej reklamy, żadnego handlu danymi, żadnego trenowania ani dostrajania (fine-tuning) modeli AI z użyciem treści lekcji. Żadnych odcisków głosu, indywidualnych profili osobowości lub osiągnięć, analizy czasu mówienia, emocji, zachowania ani obecności. Techniczna statystyka eksploatacyjna nie może umożliwiać oceny poszczególnych uczniów lub nauczycieli i nie jest przekazywana dostawcy.

Przetwarzanie podczas lekcji

5. Przepływ danych i filtr treści

1. **Aktywacja:** Nauczyciel aktywuje przetwarzanie mowy wyłącznie dla uzgodnionych fragmentów lekcji. Stan aktywny jest rozpoznawalny; zatrzymanie kończy rejestrowanie.
2. **Lokalne rozpoznawanie:** Mowa jest przekształcana w tekst na serwerze szkoły. W żadnym momencie nie powstaje zapisany plik audio, również nie do celów konserwacji ani diagnostyki błędów.
3. **Filtr przed zapisaniem:** Imiona i nazwiska z klasy, informacje prywatne i wypowiedzi niezwiązane z przedmiotem są usuwane. Należą do nich na przykład wywoływanie po imieniu, prośby o wyjście do toalety, prywatne konflikty, informacje o stanie zdrowia i organizacyjne wtrącenia bez związku z nauką.
4. **Przedmiotowa notatka edukacyjna:** Zapisywana jest oczyszczona treść przedmiotowa. Merytorycznie potrzebne nazwiska historyczne lub literackie, na przykład w temacie z historii, pozostają możliwe. Pierwotna wypowiedź osobista nie jest przechowywana obok.
5. **Wyszukiwanie i odpowiedź:** Do wyszukiwania i lokalnej AI trafiają wyłącznie dopuszczone treści uprawnionego kursu. Osobiste czaty, dzienniki bezpieczeństwa i wycofane treści nie są wspólnymi źródłami edukacyjnymi.
6. **Usuwanie:** Nieprzetworzony tekst jest odrzucany po filtrowaniu, najpóźniej pięć minut po zarejestrowaniu. Źródła i wygenerowane z nich dane wyszukiwania są usuwane po tym samym terminie ustalonym przez szkołę.

Awaria filtra nie może spowodować niefiltrowanego zapisu ani publikacji. Fragmenty, których nie można bezpiecznie przetworzyć, są odrzucane. Treści prywatne nie są również kopiowane do dzienników diagnostycznych, zbiorów danych testowych ani kopii zapasowych.

6. Opcjonalny przegląd i granice merytoryczne

Nauczyciele mogą sprawdzać, poprawiać lub usuwać notatki. Przegląd jest opcjonalny; nie ma obowiązkowego etapu zatwierdzania każdej notatki. Notatki edukacyjne mogą zatem być widoczne już przed przeglądem przez człowieka. Automatyczne filtry mogą przeoczyć informacje, a treści AI mogą być błędne lub niepełne.

Szkoła ustanawia dostępną drogę zgłoszeniową. Zgłoszone treści osobowe lub błędne są sprawdzane i w razie potrzeby blokowane, poprawiane lub usuwane, łącznie z ich danymi pochodnymi. Wskazówka o możliwych błędach AI nie zastępuje skutecznego filtrowania technicznego ani rozpatrywania zgłoszeń.

AI wspiera naukę i powtarzanie. Nie podejmuje decyzji dotyczących oceniania, promocji do następnej klasy ani przyjęcia do szkoły i nie tworzy automatycznych osobowych ocen osiągnięć. Treści lekcji oparte na źródłach i uzupełniające wyjaśnienia ogólne muszą pozostać rozróżnialne.

6.1 Ochrona wszystkich obecnych

Przed rozpoczęciem korzystania uczniowie, nauczyciele i inne osoby, których dane dotyczą, są informowani. Prywatne rozmowy są wyłączone z rejestrowania. Osoba, której dane nie mogą być rejestrowane, potrzebuje rzeczywiście skutecznego rozwiązania w pomieszczeniu; niezakładanie konta lub sama zmiana miejsca siedzenia nie wystarczają. W razie potrzeby przetwarzanie mowy pozostaje wyłączone.

Szyfrowanie

7. Wszystkie pliki chronione podczas przechowywania i przesyłania

Wszystkie pliki i dane lokalnej instalacji szkolnej są szyfrowane w stanie spoczynku (at rest) i podczas przesyłania (in transit). Wymóg ten obejmuje wszystkie miejsca przechowywania i drogi sieciowe aplikacji, łącznie z kopiami zapasowymi, plikami tymczasowymi i dostęпами administracyjnymi.

7.1 Szyfrowane nośniki danych i wolumeny danych

Fizyczne nośniki danych lub wolumeny danych są szyfrowane przed zapisaniem danych szkolnych. Obejmuje to bazy danych wraz z ich dziennikami zmian, przesłane materiały, notatki edukacyjne, indeksy wyszukiwania, dane kont, dzienniki bezpieczeństwa oraz pliki tymczasowe, o ile w ogóle mogą być tworzone. Audio i surowy tekst nie mogą przez to stać się dozwolonymi zasobami przechowywanymi.

Odpowiednimi metodami są na przykład **LUKS2 z dm-crypt w systemie Linux** lub **FileVault w systemie macOS**. Dyski zewnętrzne, dodatkowe wolumeny, kopie zapasowe, migawki (snapshoty) oraz pliki wymiany i hibernacji są uwzględniane osobno. Samo zaszyfrowanie dysku systemowego nie dowodzi, że wszystkie pozostałe miejsca przechowywania są zaszyfrowane.

Kopie zapasowe znajdują się wyłącznie na zaszyfrowanych, osobno chronionych nośnikach lokalnych. Nie ma niezaszyfrowanych kopii na nośnikach wymiennych ani automatycznej synchronizacji z chmurą. Konkretna platforma, objęte wolumeny i wybrana metoda są dokumentowane dla danej instalacji.

7.2 Szyfrowane przesyłanie

Dostęp przez przeglądarkę odbywa się przez **HTTPS/TLS**. Wszystkie pozostałe odcinki sieciowe, łącznie z połączeniem punktu mikrofonowego z serwerem szkoły, usługami wewnętrznymi przez sieć, przesyłaniem kopii zapasowych i dopuszczoną zdalną konserwacją, muszą być uwierzytelnione i szyfrowane. Certyfikaty i strony połączenia są sprawdzane; błąd nie może spowodować powrotu do niezaszyfrowanego połączenia.

Dopuszczony dostęp zdalny korzysta dodatkowo z kontrolowanego przez szkołę bezpiecznego dostępu. Sama przynależność do sieci szkolnej lub hasło do Wi-Fi nie zastępują sprawdzenia poszczególnych dróg przesyłania. Urządzenie podłączone wyłącznie fizycznie jest oceniane jako osobne przyłącze lokalne i chronione przed nieuprawnionym dostępem.

7.3 Klucze, przywracanie i ograniczenia

Szkoła wyznacza osoby odpowiedzialne za klucze i przywracanie. Klucze odzyskiwania są przechowywane oddzielnie od chronionego nośnika danych i dostępne wyłącznie dla osób uprawnionych; bez przechowywania w ogólnym obszarze dokumentów i bez niekontrolowanego składowania na prywatnym koncie w chmurze.

Podczas wdrożenia sprawdzane są zablokowane nośniki danych, ponowne uruchomienie, odblokowanie, cofnięcie uprawnień oraz przywrócenie zaszyfrowanej kopii zapasowej. Przy wymianie lub wycofaniu z użytku dane i klucze należy usunąć w sposób kontrolowany.

Szyfrowanie nośników danych chroni w szczególności zablokowany, utracony lub wymontowany nośnik pamięci. Uprawnione działające aplikacje muszą móc przetwarzać treści. Dlatego ochrona dostępu, bezpieczne urządzenia końcowe, filtrowanie treści i usuwanie pozostają dodatkowo niezbędne. Sam publiczny plik PDF nie wymaga hasła.

Dostępny i dalsze środki ochrony

8. Rola i uprawnienia

Rola	Dozwolony zakres
Uczniowie	Treści edukacyjne własnych uprawnionych kursów; własne pytania do AI, o ile zostały dopuszczone. Brak dostępu do czatów innych osób, funkcji administracyjnych lub pełnych dosłownych zapisów lekcji.
Nauczyciele	Przeglądanie treści edukacyjnych przypisanych im kursów oraz opcjonalne sprawdzanie, poprawianie lub usuwanie. Wgląd w indywidualne przebiegi zadań wymaga odrębnego, wcześniej wyjaśnionego celu szkolnego i odpowiedniego uprawnienia.
Rodzice i opiekunowie prawni	Brak automatycznego dostępu. Osobno dozwolony dostęp do odczytu jest ograniczony do przypisanych treści i nie pozwala na ogólną obserwację klasy ani rozmów innych osób.
Dyrekcja szkoły / administracja	Wyznaczone zakresy odpowiedzialności za zezwolenia, uprawnienia do kursów, blokady i uzasadnione kontrole indywidualne. Rola administracyjna nie uzasadnia analizy wszystkich interakcji edukacyjnych bez konkretnego powodu.
Dział IT szkoły	Niezbędna konserwacja techniczna, tworzenie kopii zapasowych i przywracanie z ograniczonymi uprawnieniami uprzywilejowanymi. Brak samodzielnej pedagogicznej analizy treści.
Wsparcie techniczne dostawcy	Wyłącznie konkretnie zlecony, ograniczony w czasie dostęp. Brak stałego połączenia, brak samodzielnego nadawania sobie uprawnień i brak prywatnego wykorzystywania treści lekcji.

8.1 Egzekwowanie techniczne

Uprawnienia do kursów i ról są kontrolowane na serwerze przy każdym zapytaniu, wyszukiwaniu, wyświetleniu i zmianie. Sam widoczny przycisk lub ważny dostęp nie wystarcza. Cofnięcie uprawnień kończy również istniejące sesje i dostęp do wycofanych treści.

Dane logowania są przechowywane w sposób chroniony; hasła nie są zapisywane w postaci jawnej. Dostęp uprzywilejowany otrzymują dodatkowy składnik uwierzytelniania lub równoważnie zabezpieczone procedury. Konta techniczne otrzymują wyłącznie uprawnienia niezbędne do ich zadania. Tajne dane dostępowe nie pojawiają się w treściach edukacyjnych ani w dziennikach.

8.2 Eksploatacja, urządzenia końcowe i dostępność

Serwer i nośniki kopii zapasowych znajdują się w obszarze chronionym przed nieuprawnionym wstępem. Udostępnienia sieciowe są ograniczone do niezbędnych usług; dostęp do bazy danych, modelu i pamięci masowej nie jest otwierany bezpośrednio dla uczniów ani sieci domowych. Aktualizacje bezpieczeństwa, zakresy odpowiedzialności i procedury przywracania są udokumentowane.

Odczyt i interaktywne pytania do AI są osobnymi zezwoleniami. Dostęp z domu nie umożliwia podsłuchiwanie i nie włącza mikrofonów. Aplikacja nie tworzy trwałych kopii treści w bazach danych przeglądarki ani w pamięciach podręcznych offline. Szkoły regulują kwestie bezpiecznych urządzeń końcowych i wylogowywania; zrzutom ekranu ani samodzielnie tworzonemu prywatnym kopiom nie da się w pełni zapobiec środkami technicznymi.

W przypadku awarii dostępna jest odpowiednia alternatywa edukacyjna. Nie ma automatycznego przełączania na zewnętrzne usługi AI. Nowe funkcje i zmienione drogi danych są przed aktywacją oceniane pod kątem ochrony danych.

Okresy przechowywania i usuwanie

9. Decyduje szkoła, standardem jest jeden rok szkolny

Szkoła określa okres przechowywania treści edukacyjnych. Standardem jest jeden rok szkolny: usunięcie na koniec danego roku szkolnego. W regularnym bawarskim roku szkolnym 2026/27 jest to 31 lipca 2027. Treść dodana później nie otrzymuje automatycznie kolejnych dwunastu miesięcy. Podstawą granicy roku szkolnego jest [art. 5 BayEUG](#).

Można ustalić krótszy termin. Dłuższe przechowywanie wymaga nadal dopuszczalnego i niezbędnego celu i jest wyjaśniane z góry. Samo późniejsze wywołanie treści nie przedłuża żadnego terminu. Poniższe granice są wymogami produktu; surowsze obowiązujące wymogi mają pierwszeństwo.

Zasób	Termin / zdarzenie usunięcia
Audio	Brak zapisanych plików audio, brak archiwum i brak kopii zapasowych.
Nieprzetworzony tekst	Odrzucany po filtrowaniu, najpóźniej pięć minut po zarejestrowaniu. Brak kopii zapasowej.
Treści edukacyjne i dane pochodne	Notatki, materiały, zapisane pytania/odpowiedzi oraz powiązane dane wyszukiwania: termin usunięcia ustalony przez szkołę, standardowo koniec danego roku szkolnego.
Dostępny i konta	Blokada z chwilą wygaśnięcia uprawnień; usunięcie niezbędnych danych konta najpóźniej 30 dni później.
Dzienniki bezpieczeństwa	Zdarzenia dostępu najwyżej 7 dni; szczególne zdarzenia administracyjne, takie jak zmiany uprawnień, najwyżej 30 dni. Każdorazowo bez treści lekcji ani rozmów.
Kopie zapasowe	Szyfrowane, rotacyjnie najwyżej 14 dni. Brak dalszego kopiowania do archiwum bez ograniczenia czasowego. Usunięte dane nie mogą stać się ponownie dostępne w wyniku przywrócenia.
Anonimowa statystyka eksploatacyjna	Wyłącznie rzeczywiście anonimowe wskaźniki zbiorcze, o ile szkoła na nie zezwała. Okres ustalony przez szkołę, standardowo koniec roku szkolnego; brak indywidualnej historii ani przekazywania dostawcy.

9.1 Pełny łańcuch usuwania

Przy usuwaniu treść jest najpierw wyłączana z wyświetlania, wyszukiwania i wywoływania przez AI. Następnie oczyszczane są źródło, wersje, pochodne notatki, wpisy indeksu, pliki i dopuszczalne pamięci pośrednie. Usunięcie tylko widocznej notatki nie wystarcza, jeżeli jej dane pochodne pozostają nadal dostępne.

Istniejąca kopia zapasowa może zawierać niedostępną już do użytku kopię jeszcze najwyżej 14 dni. Przed dopuszczeniem przywrócenia ponownie stosowane są usunięcia i cofnięcia uprawnień dokonane w międzyczasie. Nieudane cykle usuwania są powtarzane i kontrolowane.

Wymagane dowody prawne dotyczące zgód, zezwoleń lub przypadków naruszenia ochrony danych szkoła prowadzi osobno, zgodnie z każdorazowo obowiązującym terminem. Nie uzasadniają one ogólnego archiwum lekcji ani archiwum audio w ContextFriend.

Odbiorcy, dostęp zdalny i konserwacja

10. Brak zewnętrznego przetwarzania treści lekcji

W tej lokalnej wersji wykluczone są zewnętrzne usługi AI, magazyny w chmurze, śledzenie treści oraz wykorzystywanie danych z lekcji przez producentów mikrofonów lub modeli. Aplikacja wykorzystuje treści wyłącznie do celów ustalonych przez szkołę. Pobranie modelu lub aktualizacja oprogramowania nie przekazuje dostawcy żadnych treści lekcji.

Dostęp otrzymują wyłącznie osoby uprawnione do danego kursu i celu oraz w stosownych przypadkach wyraźnie zlecone podmioty techniczne. Szkoła wskazuje faktycznie zaangażowanych usługodawców i ich rolę w szkolnych informacjach. Dalsze podmioty przetwarzające są angażowane wyłącznie na wymaganej podstawie umownej i zgodnie z uzgodnioną procedurą zatwierdzania.

10.1 Dostęp z domu

Dostęp z domu jest dopuszczany wyłącznie przez szkołę. Połączenie prowadzi w postaci zaszyfrowanej do punktu końcowego kontrolowanego przez szkołę i otwiera jedynie dozwoloną aplikację, a nie ogólny dostęp do sieci szkolnej. Sam odczyt nie pozwala jeszcze na interaktywne pytania do AI.

Dozwolone teksty są wyświetlane na zalogowanym urządzeniu końcowym; to wyświetlanie odbywa się wówczas poza budynkiem szkoły. Operatorzy sieci mogą widzieć metadane połączenia. AI i właściwy zasób danych pozostają na serwerze szkoły. Przekazywanie treści lekcji podmiotom w państwach trzecich nie jest w tej wersji przewidziane; odmienne dostępy nie mogą być włączane po cichu.

10.2 Dostęp dostawcy wyłącznie w indywidualnych przypadkach

TamerinTECH nie ma stałego dostępu do danych z lekcji. Wsparcie techniczne jest realizowane w miarę możliwości bez dostępu do treści. Jeżeli w indywidualnym przypadku wgląd w dane jest niezbędny, szkoła ustala wcześniej cel, zleconą osobę, uprawnienia, czas trwania i dopuszczalne narzędzia. W przypadku przetwarzania danych osobowych w imieniu administratora wcześniej obowiązuje wymagana umowa o przetwarzanie w imieniu administratora (AVV, art. 28 RODO).

Zdalna konserwacja odbywa się w postaci zaszyfrowanej z zabezpieczonego, zarządzanego urządzenia wsparcia technicznego w Niemczech. Kopie treści, pobieranie, drukowanie, nagrywanie oraz przenoszenie do zewnętrznych systemów zgłoszeń lub narzędzi AI są niedozwolone. Sesja kończy się z chwilą wykonania zlecenia, upływu uzgodnionego okna czasowego lub odwołania; pozostałe uprawnienia są cofane. Jeżeli możliwości ochrony są niewystarczające, konserwacja odbywa się na miejscu.

Protokół konserwacji dokumentuje powód, uprawnioną osobę, okres i wykonane działania, bez uwzględniania treści lekcji. Wsparcie techniczne nie jest zezwoleniem na nagrywanie audio ani na tworzenie własnego zbioru testowego i treningowego. Prywatna rola szkolna pracownika dostawcy nie uzasadnia żadnych dodatkowych uprawnień dostawcy.

10.3 Kopie zapasowe i zmiany

Kopie zapasowe pozostają na osobnych, zaszyfrowanych nośnikach w ustalonym przez szkołę lokalnym obszarze chronionym. Zakres odpowiedzialności, zakres kopii zapasowych, cele przywracania i regularne testy przywracania należy dokumentować. Ryzyko awarii całej lokalizacji jest oceniane osobno; nie zezwala ono na ukrytą kopię w chmurze.

Zmiany modeli, funkcji, uprawnień, miejsc przechowywania, terminów lub odbiorców są oceniane przed ich wdrożeniem i w sposób możliwy do prześledzenia aktualizowane w informacjach. Aktualizacja nie może po cichu rozszerzać opisanej tu koncepcji ochrony.

Prawa i incydenty ochrony danych

11. Prawa osób, których dane dotyczą

Przy spełnieniu ustawowych przesłanek przysługują prawa dostępu do danych, ich sprostowania, usunięcia, ograniczenia przetwarzania oraz w stosownych przypadkach przenoszenia danych. W przypadku przetwarzania w celu wykonania zadania publicznego można wnieść sprzeciw z przyczyn związanych ze szczególną sytuacją. Udzielone zgody można wycofać na przyszłość. Właściwe zasady znajdują się w art. 12 do 22 RODO.

Szkoła będąca administratorem danych lub jej inspektor ochrony danych przyjmują wnioski. Tożsamość jest sprawdzana wyłącznie w niezbędnym zakresie. Odpowiedź następuje zasadniczo w ciągu miesiąca; o ustawowo dopuszczalnym przedłużeniu i jego przyczynach informuje się w terminie. Odmowa jest uzasadniana i opatrzona przewidzianymi informacjami o środkach ochrony prawnej.

TamerinTECH wspiera szkołę przy zleconym przetwarzaniu, ale nie podejmuje samodzielnych decyzji o udostępnieniu obcych danych z lekcji. Osoby, których dane dotyczą, nie muszą przebiegać się przez ustawienia techniczne, aby przedstawić swoją sprawę.

11.1 Możliwości składania skarg

Właściwość	Kontakt
Państwowe szkoły bawarskie	Bayerischer Landesbeauftragter für den Datenschutz (bawarski organ ochrony danych) Postfach 22 12 19, 80502 München Adres dla odwiedzających: Wagnmüllerstraße 18, 80538 München Telefon: +49 89 212672-0 poststelle@datenschutz-bayern.de www.datenschutz-bayern.de
Podmioty niepubliczne w Bawarii	Bayerisches Landesamt für Datenschutzaufsicht (bawarski urząd nadzoru ochrony danych) Postfach 1349, 91504 Ansbach Adres dla odwiedzających: Promenade 18, 91522 Ansbach Telefon: +49 981 180093-0 poststelle@lda.bayern.de www.lda.bayern.de

W przypadku innych organów prowadzących lub szczególnych właściwości szkoła wskazuje właściwy organ nadzorczy. Urzędy te oferują bezpieczne formularze online do składania skarg. Punkt kontaktowy u dostawcy i organ nadzorczy to różne podmioty.

12. Błędy i incydenty bezpieczeństwa

Niezamierzone ujawnienie, nieuprawniony dostęp, utrata lub inne naruszenia ochrony danych są niezwłocznie zgłaszane szkolną drogą zgłoszeniową. Właściwe podmioty ograniczają dostęp, zabezpieczają niezbędne dowody o minimalnej treści oraz badają skutki i środki zaradcze. Dotknięte treści edukacyjne są w razie potrzeby blokowane.

Administrator danych bada kwestię zgłoszenia do organu nadzorczego zgodnie z art. 33 RODO, zasadniczo w ciągu 72 godzin od stwierdzenia naruszenia, o ile istnieje obowiązek zgłoszenia. W przypadku prawdopodobnego wysokiego ryzyka osoby, których dane dotyczą, są informowane zgodnie z art. 34 bez zbędnej zwłoki. Podmiot przetwarzający informuje administratora danych niezwłocznie po stwierdzeniu naruszenia.

Ponowne uruchomienie i przywrócenie następują dopiero po sprawdzeniu środków ochrony, uprawnień i wymogów dotyczących usuwania. Awaria nie uzasadnia ani nagrywania dźwięku, ani niekontrolowanego przekazywania danych szkolnych.

Wiążący charakter i źródła

13. Wdrożenie w szkole i utrzymywanie dokumentów

Dla każdej szkoły muszą być ustalone faktyczny stan dostawy, funkcje, urządzenia, modele, drogi danych, terminy i właściwe podmioty. Szkoła sporządza swoje konkretne informacje oraz wymagany rejestr czynności przetwarzania. Bada obowiązek przeprowadzenia oceny skutków dla ochrony danych; jeżeli ocena skutków (DSFA) jest wymagana, musi zostać zakończona przed rozpoczęciem przetwarzania. Pozostałe wysokie ryzyko należy traktować zgodnie z art. 36 RODO.

Podczas wdrożenia w każdej instalacji sprawdzane i dokumentowane są w szczególności: brak zapisu audio również w przypadku błędów, filtrowanie przed zapisaniem, granica pięciu minut dla surowego tekstu, szyfrowanie wszystkich dróg przechowywania i przesyłania, skuteczne uprawnienia do kursów, poprawianie i wycofywanie oraz usuwanie łącznie z kopiami zapasowymi. Brak obowiązkowego przeglądu przez nauczycieli należy wyraźnie uwzględnić w ocenie ryzyka.

Dyrekcja szkoły decyduje o wdrożeniu wraz z właściwymi organami szkolnymi. Osoby, których dane dotyczą, są informowane przed rozpoczęciem; wymagane zgody są uzyskiwane osobno. Należy zapewnić kompetencje merytoryczne i dostosowane do wieku wsparcie przy korzystaniu z AI. Niniejsza koncepcja nie zawiera żadnego państwowego zapewnienia o dopuszczeniu ani o dofinansowaniu.

Wersja 1.3 z 16 października 2026 obowiązuje łącznie z wersją skróconą o tej samej dacie. Zmiany są dokumentowane w sposób możliwy do prześledzenia. Publiczne pliki PDF nie zawierają wypełnionych dokumentów szkolnych, umownych ani wniosków. Szkoła otrzymuje potrzebne jej dokumenty umowne i eksploatacyjne osobno.

14. Źródła prawne i specjalistyczne

1. [Ogólne rozporządzenie o ochronie danych \(RODO\)](#), w szczególności art. 5, 6, 9, 12 do 22, 25, 28, 30, 32 do 39.
2. [art. 85 BayEUG](#) o przetwarzaniu danych osobowych; [art. 5 BayEUG](#) o granicy roku szkolnego.
3. [§ 46 BaySchO z załącznikiem 1](#) o szkolnych czynnościach przetwarzania; dalsze przepisy właściwe dla danej szkoły pozostają do zbadania.
4. [Bayerisches Kultusministerium \(bawarskie ministerstwo oświaty\): sztuczna inteligencja](#), wraz z przewodnikiem praktyki pedagogicznej z 19 maja 2026.
5. [§ 38 BDSG](#) o wyznaczaniu inspektorów ochrony danych w podmiotach niepublicznych; badanie należy przeprowadzić niezależnie od niniejszej informacji kontaktowej.
6. [Dokumentacja jądra Linux: dm-crypt](#) oraz [cryptsetup/LUKS](#); [Apple: FileVault](#). Opisy procedur nie zastępują sprawdzenia instalacji.
7. Źródła kontaktowe: [Impressum ContextFriend](#), [BayLfD](#) oraz [BayLDA](#). Stan na dzień pobrania: 14 października 2026.

Kontakt w sprawach ochrony danych u dostawcy

TamerinTECH GmbH · Seestr. 19 · 83727 Schliersee · Niemcy
hello@context-friend.com · +49 8026 387 25 98

W sprawach danych z lekcji prosimy zwracać się do szkoły będącej administratorem danych lub do jej inspektora ochrony danych. Uproszczona informacja dla rodzin i niniejsza pełna koncepcja ochrony danych są dostępne pod adresem context-friend.com/school-documents.